METHOD OF TESTING THE ENCRYPTION FUNCTION OF A DEVICE

Sajosh Janarthanam

Kheng Guan (Nigel) Tan

ABSTRACT

A packet data string is provided to a device under test (DUT), which preprocesses the packet data string, based on static inputs, to provide packet segment data strings, which are placed in a queue in a memory structure. Separate therefrom, a packet segment data string is applied to an encryption engine of the DUT, which encryption engine has an initialization vector applied thereto, and an encryption algorithm of the encryption engine is applied to this packet segment data string to provide an encrypted packet segment data string. Bit length and initialization vector matching techniques are used to eliminate packet segment data strings in the queue from further consideration, and after bit length and initialization vector matching are achieved in regard to a packet segment data string in the queue, such packet segment data string is encrypted using the encryption algorithm and an initialization vector extracted from the previously encrypted packet segment data string, whereupon a bitwise comparison is made between the encrypted packet segment data strings.